

AMENDMENTS TO THE CLAIMS

This listing of claims replaces all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) A method for ensuring that data generated by a client, comprising a first computing device, and subsequently stored in a persistent storage of the client have not been modified when the data are subsequently accessed for use by the client, the method comprising:

the client computing a first digest from the data;

~~[[a]]~~—the client sending the first digest ~~data-related information~~ to a server for signature computation;

~~[[b]]~~—the server, comprising a second computing device, computing a signature for the first ~~data-related information~~ digest by utilizing a secure signing algorithm and a key, the key known only by the server and available for use only by the server; ~~that is only known and available for use by the server;~~

~~[[c]]~~—the server sending the signature to the client for storage;

~~[[d]]~~—the client storing both the signature and the data in the persistent storage of the client;

~~[[e]]~~—before the stored data ~~that were stored are being~~ subsequently used by the client, the client computing a second digest from the stored data;

the client sending both the second digest ~~data-related information~~ and the previously stored signature to the server to verify that the stored data ~~that were stored have~~ has not been changed;

the server receiving both the second digest and the previously stored signature;

~~[[f]]~~—the server generating a temporary signature of the second digest ~~data-related information~~ by utilizing the secure signing algorithm and the key known only by the server and available for use only by the server; ~~that is only known and available for use by the server;~~

~~[[g]]~~—the server comparing the temporary signature to the previously stored signature;

~~[[h]]~~—when the temporary signature is equal to the previously stored signature, the server sending a positive result to the client;

~~[[i]]~~—when the temporary signature is not equal to the stored signature, the server sending a negative result to the client.;

~~— [[j]] the client receiving the result from the server and evaluating the result;~~

~~— [[k]] when the result is positive, the client using the data; and~~

~~— [[l]] when the result is negative, the client not using the data.~~

2 – 4. (Canceled)

5. (Currently Amended) The method of Claim 1, wherein the first digest~~data-related information~~ comprises a digest of the data calculated by the client using a one-way hash function and the data, and the second digest~~data-related information~~ comprises a digest of the stored data calculated by the client using a one-way hash function and the stored data.

6 – 7. (Canceled)

8. (Currently Amended) The method of Claim 5, wherein the first digest~~data-related information~~ further comprises:

~~[[a]]~~—a signer identification (SID) for the client, the SID uniquely identifying the client and not being controlled by an operator of the client;

9 – 10. (Canceled)

11. (Currently Amended) The method of Claim 1, wherein the data comprise a plurality of different sets of data, and the method further comprising: ~~the steps of:~~

~~[[a]]~~—obtaining a signer identification (SID) for the client, the SID uniquely indicating the client and not being controlled by an operator of the client;

~~[[b]]~~—on the server, using the key for computing an intermediate key from a concatenation of an arbitrary value and the SID;

~~[[c]]~~—sending the intermediate key from the server to the client;

~~[[d]]~~—using the intermediate key to sign each set of the data to produce the signature for the set of data; and

~~[[e]]~~—storing the signature, the arbitrary value, and the SID on the persistent storage.

12 – 13. (Canceled)

14. (Currently Amended) The method of Claim 11, further comprising ~~the step of~~ determining if the SID that was received from the client is on a list of banned SIDs, and if so, indicating in the result that the set of data are not usable by the client.

15 – 18. (Canceled)

19. (Currently Amended) A computer program product comprising a computer memory medium on which are stored machine readable instructions which, when executed on one or more computer processors, perform the method of claim 1. ~~are stored for carrying out the steps of Claim 1.~~

20 – 36. (Canceled)